

# Architecture Concepts For A Future Heterogeneous, Survivable Tactical Internet

---

Dr. John Chapin  
Program Manager  
Strategic Technology Office  
[john.chapin@darpa.mil](mailto:john.chapin@darpa.mil), 703-248-1533

Symposium: Novel Methods for Information Sharing in  
Large-scale Mobile Ad-hoc Networks

August 8, 2013





# Scope of 2012 DARPA/STO network architecture study

---

## Internetworking layer and services

Services available in all modalities (wired, wireless, optical, SATCOM, ...)

Data and control functions that coordinate and integrate subnets

## Fundamental design features appropriate for multiple modalities / environments

### Out of scope:

Network designs for specific modalities / operational environments

*Internetworking layer should enable deploying such networks faster than today, with better GIG integration.*



# Rationale for a new internetworking architecture

---

## Military utility of current Internet

- Support strategic operations
- Survive a nuclear attack

## Military goals for this study

- Support tactical and theater operations
- Survive close contact with a peer adversary

## Environment of current Internet

- Wired network
- Constrained resource
  - Link bandwidth

## Environment for this study

- Heterogeneous network
- Constrained resource varies by situation
  - Link bandwidth
  - Spectrum
  - Power consumption
  - Detectability
  - Latency

This is a different target than the NSF FIA projects

Used with permission. The views expressed are those of the author and do not reflect the official policy or position of DARPA, the Department of Defense, or the U.S. Government.



# Detail on new military goals

---

## Support tactical operations

- Rapid change in environmental attributes

- Limited support personnel

- Mission critical communications (time deadline delivery)

## Survive close contact with peer adversary

- Jamming from adversary or from blue EW

- Targeting on and exploitation of transmissions

- Destruction of relays/gateways

- Cyber penetration of some nodes



# New Internet-layer services

---

A **service** consists of a network stack and implementations of core functions (naming, authentication, control) needed to support application information exchange.

## Examples

**Hard Core:** Maximize probability of on-time delivery

Proactively provision multiple paths between nodes.  
Increase resources deadline is at risk.  
Use Byzantine or attack resilient algorithms at all layers.

**AJ:** Survive adversary jamming

Spread information over data stream to minimize vulnerability of high-leverage bits or packets.

**LPD:** Survive adversary targeting/exploitation of transmissions

Employ low duty cycle, sporadic data transfers with unpredictable timing.

**Asymmetric:** Connect LPD to unconstrained nodes

e.g. Relays outside threat zone

**Elephant:** Efficient support for large transfers

## Multi-service network requirements

- One node accesses multiple services
- Multiple services active at the same time
- Data flows can transit multiple services

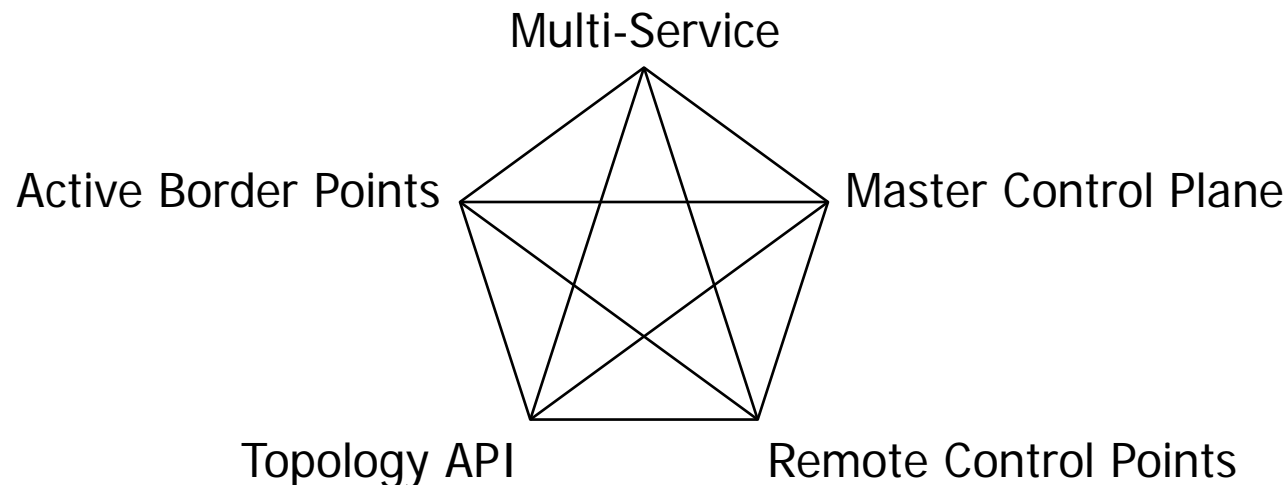


## Goal: a coherent internetwork architecture

What does an internetwork look like that has these properties?

While remaining efficient, evolvable, secure, ...

The study identified 5 architectural components that can work together to achieve this.

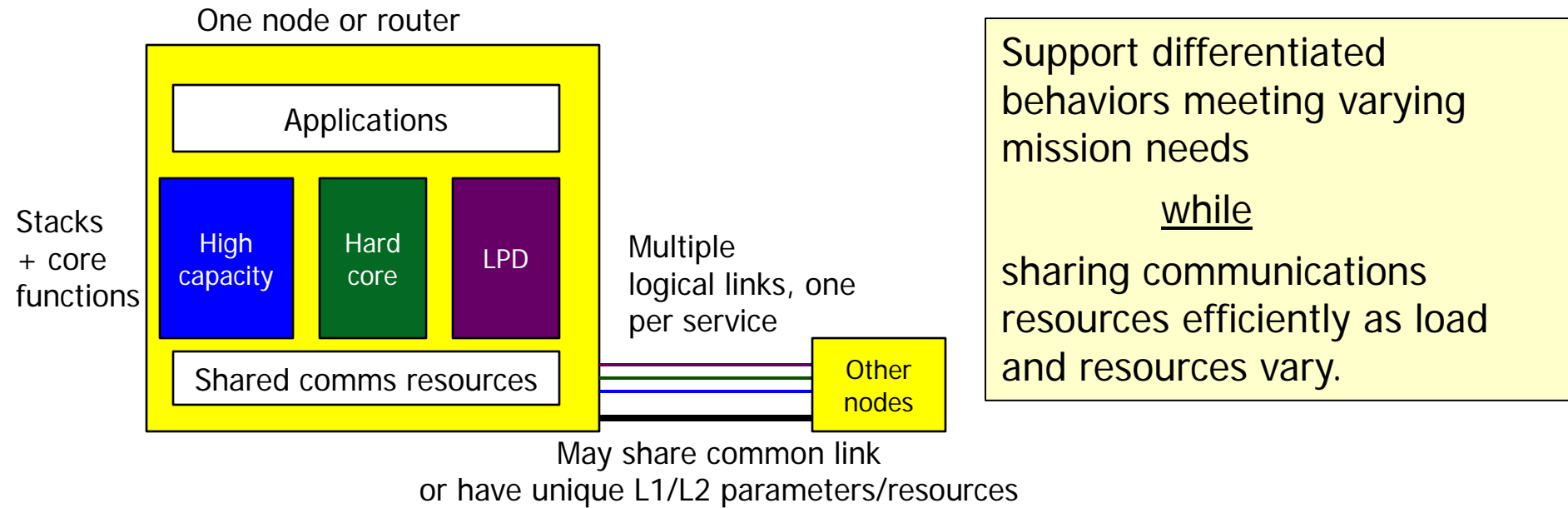


Individually these ideas are not new.

The opportunity is the synergy among them in a greenfield coherent architecture.



# Multi-service: enable multiple services to coexist

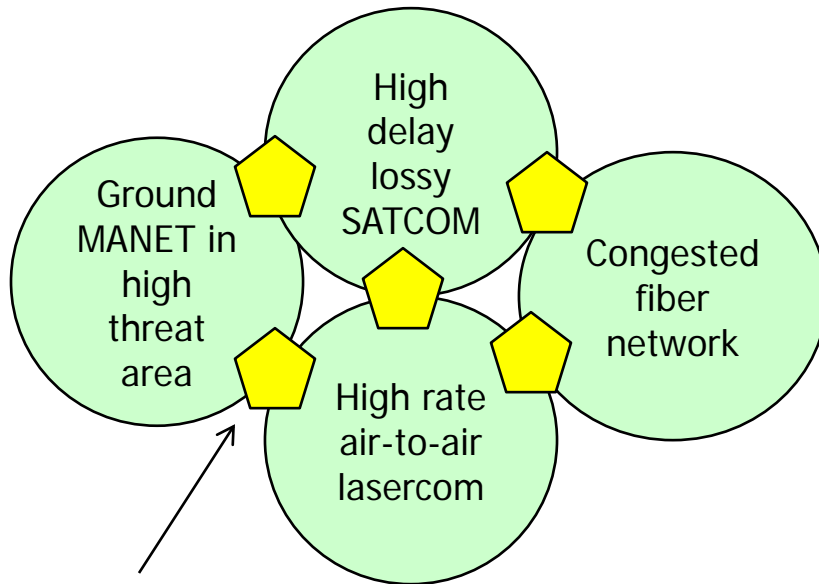


## Research gaps:

- coexistence/sharing mechanisms enabling multiple services
- security isolation between services
- control mechanisms to manage resource allocation among services



# Multi-service: Active Border Points



Current Internet architecture assumes the junction between subnets is a wire.

In DOD nets the junction is a computer or subsystem, so make it part of the architecture: **Active Border Point**

Expose Border Points to applications/middleware.

Functions:

- Transport protocol segmentation
- Remote control point
- Security/congestion monitoring and isolation

Used with permission. The views expressed are those of the author and do not reflect the official policy or position of DARPA, the Department of Defense, or the U.S. Government.

Allow subnets to differ from each other much more than they do today

while

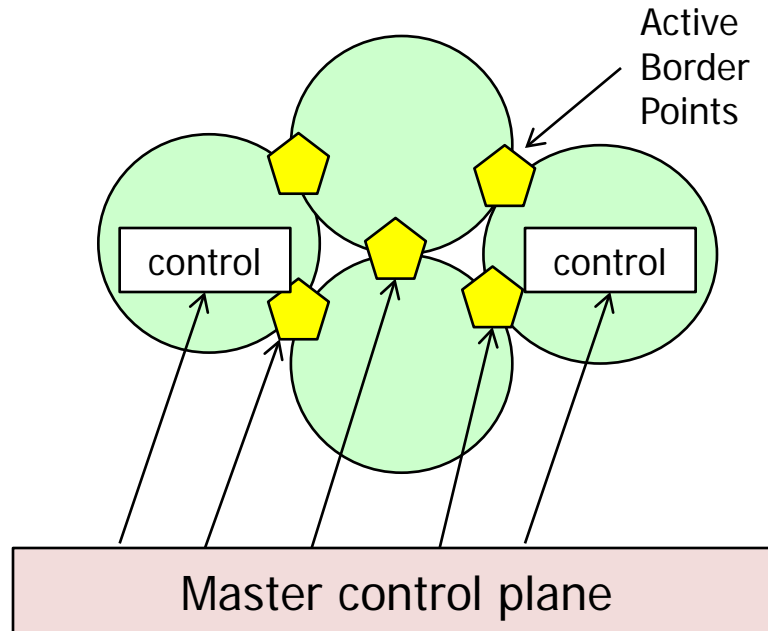
coordinating the subnets more closely to achieve enterprise level goals.

Research gaps:

- scalable segmented transport mechanism with rerouting
- detection of faulty subnets
- security isolation between subnets



# Global coordination: Master Control Plane



Optimize global routing, security, management via a Master Control Plane:

- Coordinate among subnet control systems
- Monitor/control Active Border Points

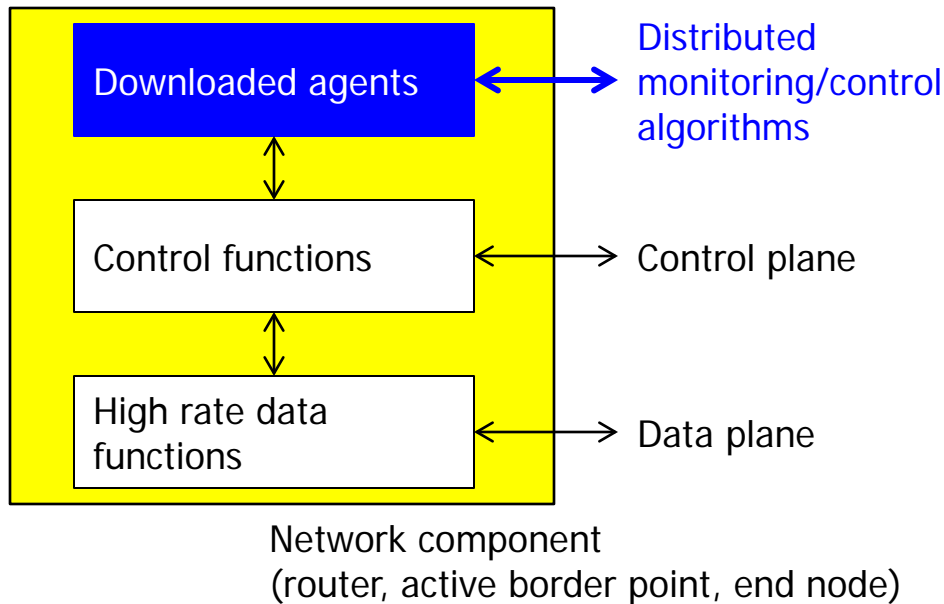
Provide enterprise-level optimization and management while preserving local control of each subnet.

Research gaps:

- distributed global coordination of local control loops
- standard interface to local control planes and management



# Modular & evolvable: Remote control points



Network components download agents for modular addition of

- Distributed monitoring/control functions
- Network-aware middle layers
  - CBMEN, DTN, segmented transport

Agents access control/data plane via an API that protects network security and evolvability.

Support distributed and application-specific monitoring and control while maintaining evolvability and security.

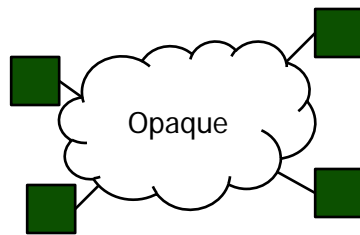
## Research gaps:

- Flow naming
- Control authorization
- Statistical representations of key parameters
- Abstract control mechanisms
- Execution environment for agents with:
  - portability
  - security
  - communications to peers
  - scalability between low- and high-capability platforms

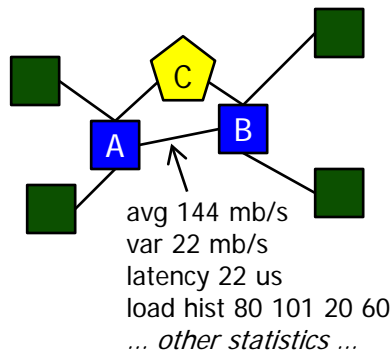
Used with permission. The views expressed are those of the author and do not reflect the official policy or position of DARPA, the Department of Defense, or the U.S. Government.



# Modular & evolvable: Topology API



Network as seen by  
current applications



Network as seen by  
application or transport  
using the Topology API

Expose relevant dynamically  
changing network state  
while  
maintaining abstraction  
boundaries and security.

Expose topology, capacity, load information

Support:

- Network-aware applications
- Network-aware middle layers
- Control systems outside the network
  - Autonomous provisioning
  - Control of L1/L2 settings to optimize topology

Research gaps:

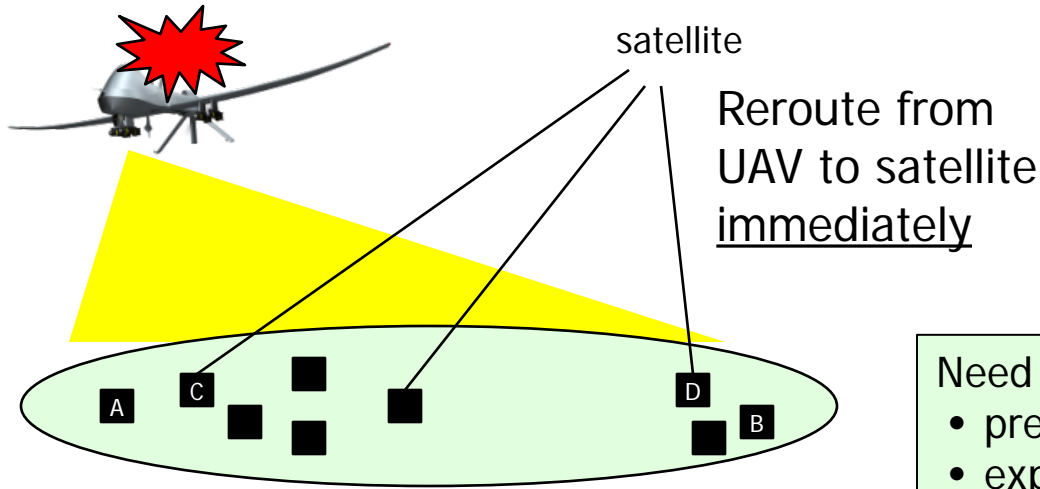
- abstract description
- naming mechanisms
- statistical representations of key parameters
- mitigation of security vulnerabilities
- efficient information collection
- efficient query mechanisms



New behaviors to be implemented on top of  
the new architecture



# Stabilized rapid adaptation



Current Internet layers reacts slowly in order to maintain stability.

Rapid adaptation is required for dynamic operational environments.

- Use active control loops to stabilize.

React rapidly to changes in  
assets, environment or goals  
while  
maintaining stability.

Need mechanisms to:

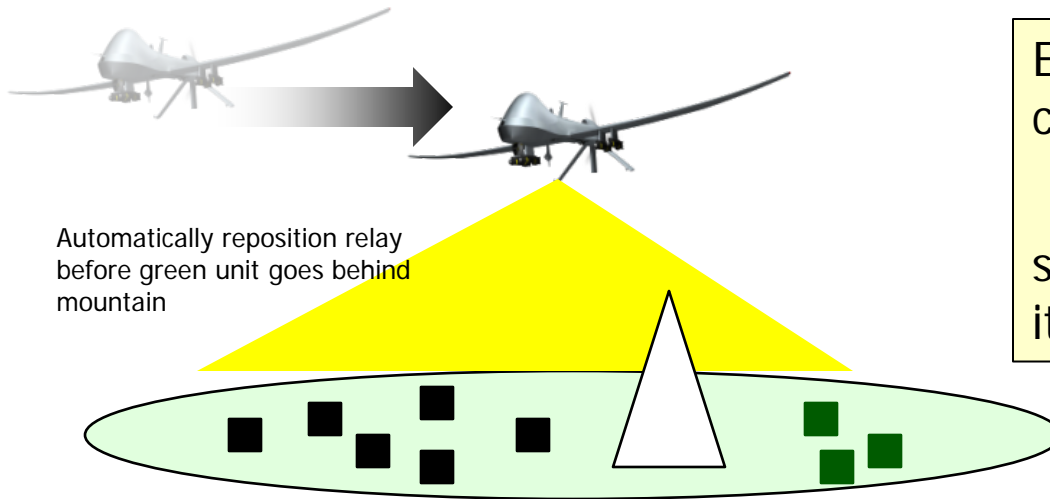
- preplan then rapidly activate
- expose L1/L2 dynamic changes to L3/L4, while preserving abstraction
- rapidly adapt L3/L4 behaviors

Need control theory for systems with:

- too many variables to measure
- operating away from equilibrium
- multiple distributed control loops
- random time delays
- plant response function changes based on external conditions



# Autonomous control



Employ distributed autonomous control and provisioning while simplifying the network and making it more evolvable.

Autonomous control is essential to:

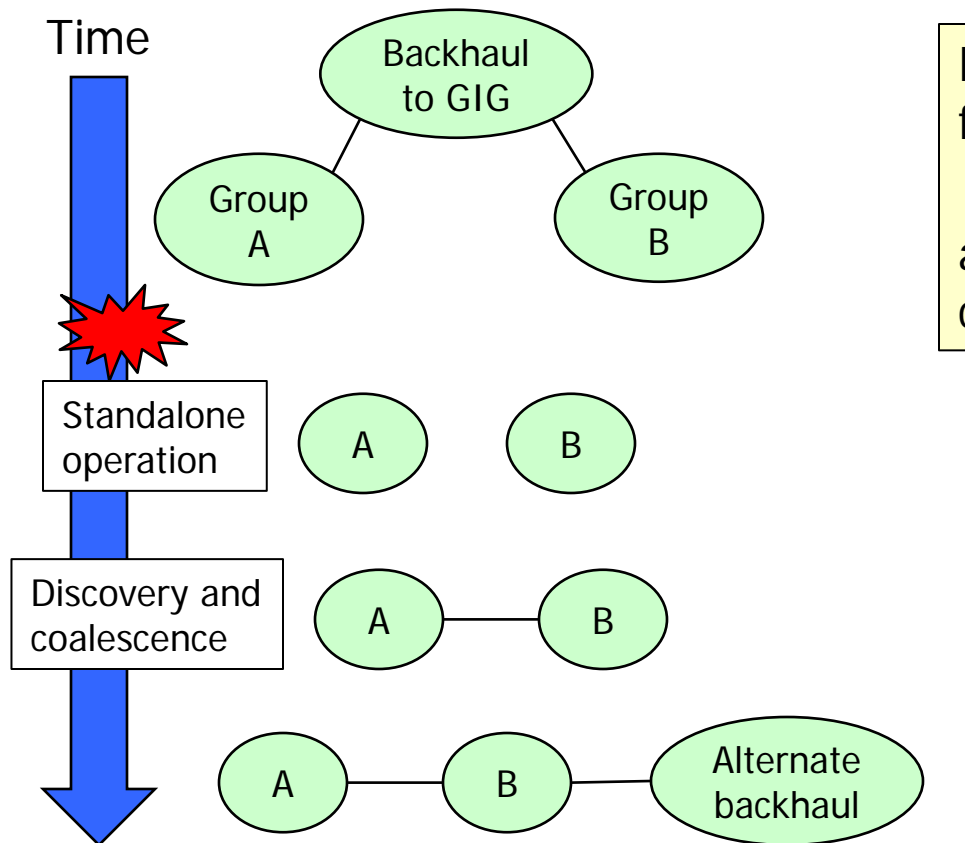
- reduce personnel requirements
- accelerate reactions in dynamic complex environments
- improve resource utilization
- enable rapid deployment
- re optimize after major environmental or asset change

Research gaps:

- Use modeling (of environment, applications, threats) to reduce required communication, reduce response latency, detect anomalies.
- Common language for statistical representations supporting interaction among control systems, learning, and anomaly detection.
- Perform resource allocation and reconfiguration based on mission goals and changing policies.



# Standalone fragments / Reconstitution



Current Internet keeps data routing alive in each fragment, but other core functions fail:

- Name resolution
- Authentication and encryption
- Control

Reconstitution is slow and manual.

Enable standalone fragments to keep fighting and to coalesce while achieving the efficiency of centralized control when coalesced.

## Gaps:

- Fully distributed implementations of (degraded modes of) core functions, or network designs that eliminate the need for those functions.
- Automatic discovery and coalescence mechanisms.
- Optimize reconstitution through exploiting a broad-area resilient low-rate "heartbeat" subnet where available (e.g. protected SATCOM).

Used with permission. The views expressed are those of the author and do not reflect the official policy or position of DARPA, the Department of Defense, or the U.S. Government.



Agree? Disagree?

How would you rearchitect the Internet layer to survive close contact with a peer adversary?

Come tell us about it at the next DARPA/STO Novel Methods Symposium.

POC: John Chapin

john.chapin@darpa.mil

703-248-1533